Weapons of Mass Disruption

Are Your Information Systems at Risk?

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

Today's Climate

- Highly interactive environment of powerful computing devices and interconnected systems of systems across global networks
- Federal agencies routinely interact with industry, private citizens, state and local governments, and the governments of other nations
- The complexity of today's systems and networks presents great security challenges for both producers and consumers of information technology

The Advantage of the Offense

- Powerful attack tools now available over the Internet to anyone who wants them
- Powerful, affordable computing platforms to launch sophisticated attacks now available to the masses
- Little skill or sophistication required to initiate extremely harmful attacks
- *Result: The sophistication of the attack is growing, but the sophistication of the attacker is not.*

Today's Challenges

- Adequately protecting information systems within constrained budgets
- Changing the current culture of:

  "Connect first…ask questions later"
- Bringing standards to:
  - the specification of security controls for information systems; and
  - the verification procedures employed to assess the effectiveness of those controls

Assurance in Information Systems

Building more secure systems requires --

- Well defined system-level security requirements and security specifications
- Well designed component products
- Sound systems security engineering practices
- Competent systems security engineers
- Appropriate metrics for product/system testing, evaluation, and assessment
- Comprehensive system security planning and life cycle management

Supporting Tools and Programs

Building more secure systems is enhanced by --

- Standardized Security Requirements and Specifications
  - ✓ Government-sponsored protection profile development project
  - ✓ Private sector protection profile contributions
- Component-level Product Testing and Evaluation Programs
  - ✓ NIAP Common Criteria Evaluation and Validation Scheme
  - ✓ NIST Cryptographic Module Validation Program
- Security Implementation Guidance
  - ✓ NIST Special Publications
  - ✓ DoD Security Technical Implementation Guides
  - ✓ NSA Security Reference Guides
- System Certification and Accreditation

The Security Chain

Links in the Chain
(Non-technology based examples)

- ✓ Physical security
- ✓ Personnel security
- ✓ Procedural security
- ✓ Risk management
- ✓ Security policies
- ✓ Security planning
- ✓ Contingency planning

Links in the Chain
(Technology based examples)

- ✓ Access control mechanisms
- ✓ Identification and authentication devices
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls
- ✓ Smart cards
- ✓ Biometrics

Adversaries attack the weakest link…where is yours?

National Policy

Office of Management and Budget Circular A-130, *Management of Federal Information Resources* requires Federal agencies to:

- Plan for security
- Ensure that appropriate officials are assigned security responsibility
- Authorize system processing prior to operations and periodically, thereafter.

The Big Picture

Information Security Program

SP 800-30

Risk Assessment

Analyzes the threats to and vulnerabilities of information systems and the potential impact or magnitude of harm that the loss of confidentiality, integrity, or availability would have on an agency's operations and assets

FIPS 199 SP 800-60

Categorization of Information and Information System

Defines categories of information and information systems according to levels of risk for confidentiality, integrity, and availability; maps information types to security categories

SP 800-18

Security Planning

Documents the security requirements and security controls planned or in place for the protection of information and information systems

AGENCY INFORMATION AND INFORMATION SYSTEM

SP 800-37 SP 800-53A

Verification of Security Control Effectiveness (Certification)

Measures the effectiveness of the security controls associated with information systems through security testing and evaluation

SP 800-53 (Interim)

FIPS 200 (Final)

Security Control Selection and Implementation

Management, operational, and technical controls (i.e., safeguards and countermeasures) planned or in place to protect information and information systems

SP 800-37

Security Authorization (Accreditation)

The authorization of information systems to process, store, or transmit information, granted by a senior agency official, based on the effectiveness of security controls and residual risk

Categorization Standards

- Develop standards to be used by agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Project underway at NIST to develop:
  - ✓ Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"
  - ✓ Public Review Period: May 16th—August 16th 2003
  - ✓ Final Publication NLT December 2003

FIPS Publication 199

- Establishes standards to be used by agencies to ***categorize*** information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels

Result

- Agencies will have a standard means of determining what baseline security controls are needed to adequately protect the information and information systems that support the operations and assets of the agency in order to:
  - accomplish its assigned missions
  - protect its assets
  - maintain its day-to-day functions
  - protect individuals

Security Objectives

- Confidentiality
  - ✓ "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]
- Integrity
  - ✓ "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]
- Availability
  - ✓ "Ensuring timely and reliable access to and use of information…" [44 U.S.C., Sec. 3542]

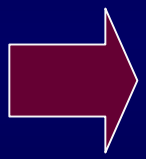
Potential Impact

- The potential impact is low if—
  - *The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.*
- The potential impact is moderate if—
  - *The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.*
- The potential impact is high if—
  - *The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.*

Security Categorization

An Example: Mission Critical Information and Information System

Guidance for Mapping Types of Information and Information Systems to FIPS Pub 199 Security Categories



	Low	Moderate	High
Confidentiality	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

National Institute of Standards and Technology

Security Categorization

An Example: Mission Critical Information and Information System

Guidance for Mapping Types of Information and Information Systems to FIPS Pub 199 Security Categories

	Low	Moderate	High
Confidentiality	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adver n organ perations, organi ssets, or individ
Availability	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The dis access to or use ation or an inform em could be e have a **severe or hic** adverse effect organizational ope organizational assets, or individuals.

Baseline Security Controls for High Impact Systems

National Institute of Standards and Technology

Mapping Guidelines

- Develop guidelines recommending the types of information and information systems to be included in each category described in FIPS Publication 199—
- Project underway at NIST to develop:
  - ✓ Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categorization Levels"
  - ✓ Initial Public Draft (Projected for publication, Fall 2003)

Minimum Security Requirements

- Develop minimum information security requirements (i.e., management, operational, and technical security controls) for information and information systems in each such category—
- Project underway at NIST to develop:
  - ✓ Federal Information Processing Standards (FIPS) Publication 200, "Minimum Security Controls for Federal Information Systems"*
  - ✓ Final Publication NLT December 2005

* NIST Special Publication 800-53, "Guide for the Selection and Specification of Security Controls for Federal Information Systems", (Initial public draft projected for publication, Fall 2003), will provide interim guidance until completion and adoption of FIPS Publication 200.

Special Publication 800-53

Guide for the Selection and Specification of Security Controls for Federal Information Systems

- Provides a catalog of security controls for information systems (incorporated from many sources (NIST SP 800-26, DoD Policy 8500, D/CID 6-3, ISO/IEC 17799, GAO FISCAM, HHS-CMS)
- Recommends baseline security controls for information systems (in accordance with FIPS Publication 199)
- Provides guidelines for agency-directed tailoring of baseline security controls

Security Controls

- Management Controls
  - Controls that address the security management aspects of the IT system and the management of risk for the system
- Operational Controls
  - Controls that address the security mechanisms primarily implemented and executed by people (as opposed to systems)
- Technical Controls
  - Controls that address security mechanisms contained in and executed by the computer system

Security Control Robustness

- Three levels of security control robustness defined (i.e., basic, enhanced, strong) based on increasing strength of mechanism and assurance of effectiveness of implementation
- Assurance defined by quality of security control design, development methodology, maturity of development processes, and rigor of testing and evaluation conducted

Security Control Example

Class: Management ***Family: Security Control Review***

CR-2 **VULNERABILITY SCANNING**

Control objective: Procedures and mechanisms are in-place and being effectively implemented to periodically scan for vulnerabilities.

CR-2.b Basic control: Vulnerability assessment tools are implemented by the agency; procedures are developed for the implementation of the assessment tools and agency personnel are trained in their use. The agency conducts periodic testing of the security posture of the information system by scanning the system with vulnerability detection tools every [*Assignment: time-period; for example, every 6 months*].

Security Control Example

Class: Management ***Family: Security Control Review***

CR-2 **VULNERABILITY SCANNING**

Control objective: Procedures and mechanisms are in-place and being effectively implemented to periodically scan for vulnerabilities.

CR-2.e Enhanced control: Vulnerability assessment tools are implemented by the agency; procedures are developed for the implementation of the assessment tools and agency personnel are trained in their use. The agency conducts periodic testing of the security posture of the information system by scanning the system with vulnerability detection tools every [*Assignment: time-period; for example, every 6 months*]. Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned. The list of vulnerabilities scanned is updated periodically, at least prior to each periodic scan. Vulnerability scanning procedures include vulnerability list update and vulnerability scan when a significant, new vulnerability is announced.

Security Control Example

Class: Management ***Family: Security Control Review***

CR-2 **VULNERABILITY SCANNING**

Control objective: Procedures and mechanisms are in-place and being effectively implemented to periodically scan for vulnerabilities.

CR-2.s Strong control: Vulnerability assessment tools are implemented by the agency; procedures are developed for the implementation of the assessment tools and agency personnel are trained in their use. The agency conducts periodic testing of the security posture of the information system by scanning the system with vulnerability detection tools every [*Assignment: time-period; for example, every 6 months*]. Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned. The list of vulnerabilities scanned is updated periodically, at least prior to each periodic scan. Vulnerability scanning procedures include vulnerability list update and vulnerability scan when a significant, new vulnerability is announced. Vulnerability scanning procedures include means to ensure adequate scan coverage, both vulnerabilities checked and information resources scanned.

Baseline Security Controls

- Three sets of baseline (minimum) security controls defined for security categories in accordance with FIPS Publication 199
- Starting point for agencies and communities of interest in their security control selection process
- Baseline security controls can be tailored by agencies based on results of risk assessments and specific security requirements (e.g., HIPAA, Gramm-Leach-Bliley)

Taxonomy of Security Controls

- Master catalog of security controls (approximately 175 entries)
- Organized by classes and families
- Includes three levels of security control robustness (basic, enhanced, and strong) when appropriate and technically feasible
- Dynamic in nature allowing revisions and extensions to security controls to meet changing requirements and technologies

Mapping Security Requirements

- Determining compliance to security requirements derived from laws, Executive Orders, directives, policies, or regulations (e.g., HIPAA) starts with a mapping of requirements to security controls
- Selected security controls can be implemented within information systems
- Effectiveness of the security controls can be verified during security certification process—leading to security accreditation (authorization to operate the information system

Certification and Accreditation

- Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical controls)
- Project underway at NIST to develop:
  - ✓ Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"
  - ✓ Special Publication 800-53A, "Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems"

Security Accreditation

"An official management decision to authorize operation of an information system—

This authorization, given by a senior agency official, is applicable to a particular environment of operation, and explicitly accepts the level of risk to agency operations (including mission, functions, image or reputation), agency assets, or individuals (including privacy), remaining after the implementation of an agreed upon set of security controls…"

National Institute of Standards and Technology

Security Certification

"A comprehensive evaluation of the technical, management, and operational security controls in an information system—

This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the vulnerabilities in the information system after the implementation of such controls…"

National Institute of Standards and Technology

Special Publication 800-37

Guide for the Security Certification and Accreditation of Information Systems

- Establishes guidelines (including tasks and subtasks) to certify and accredit information systems supporting the executive branch of the Federal government
- Applicable to non-national security information systems as defined in the Federal Information Security Management Act of 2002
- Replaces Federal Information Processing Standards (FIPS) Publication 102

Security Certification and Accreditation Process

A Four-Phase Process:

- Initiation Phase
- Certification Phase
- Accreditation Phase
- Continuous Monitoring Phase

Special Publication 800-53A

Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems

- Provides standardized techniques and procedures for independent certification agents to verify the effectiveness of security controls
- Provides a single baseline verification procedure for each security control in SP 800-53
- Allows additional verification techniques and procedures to be applied at the discretion of the agency

The Big Picture

Information Security Program

SP 800-30

Risk Assessment

Analyzes the threats to and vulnerabilities of information systems and the potential impact or magnitude of harm that the loss of confidentiality, integrity, or availability would have on an agency's operations and assets

FIPS 199 SP 800-60

Categorization of Information and Information System

Defines categories of information and information systems according to levels of risk for confidentiality, integrity, and availability; maps information types to security categories

SP 800-18

Security Planning

Documents the security requirements and security controls planned or in place for the protection of information and information systems

AGENCY INFORMATION AND INFORMATION SYSTEM

SP 800-37 SP 800-53A

Verification of Security Control Effectiveness (Certification)

Measures the effectiveness of the security controls associated with information systems through security testing and evaluation

SP 800-53 (Interim)

FIPS 200 (Final)

Security Control Selection and Implementation

Management, operational, and technical controls (i.e., safeguards and countermeasures) planned or in place to protect information and information systems

SP 800-37

Security Authorization (Accreditation)

The authorization of information systems to process, store, or transmit information, granted by a senior agency official, based on the effectiveness of security controls and residual risk

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Manager
Dr. Ron Ross
(301) 975-5390
rross@nist.gov

Assessment Scheme
Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Special Publications
Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Organization Accreditations
Patricia Toth
(301) 975-5140
patricia.toth@nist.gov

Gov't and Industry Outreach
Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Technical Advisor
Gary Stoneburner
(301) 975-5394
gary.stoneburner@nist.gov

Comments to: sec-cert@nist.gov
World Wide Web: http://csrc.nist.gov/sec-cert